United States Department of State

Office of the Director of U.S. Foreign Assistance (F)

Foreign Assistance Coordination and Tracking System (FACTS) Info

User Access Policy

August 1, 2011

Submitted by

Program Management Office (F/PM)

DOCUMENT CHANGE HISTORY

The table below identifies all changes that have been incorporated into this document.

Change #	Date	Version #	Description
N/A	May/08	Draft v1.0	FACTS Info User Access Policy Initial Working Draft
0001	June/08	Draft v2.0	Comments incorporated from Internal F/SIME Initial Review
0002	July/08	Draft v3.0	Comments incorporated from State/Legal Office
0003	October/08	Draft v4.0	Comments and Clearance from F Senior Staff
0004	October/08	Draft v5.0	Comments and Clearance from F/PM
0005	November/08	Final v1.0	Comments and Clearance from F/DCOO
0006	August/11	Final v 1.1	Updates to user agreement and POAM revisions

TABLE OF CONTENTS

1. INTRODUCTION……..…… 1

2. FACTS INFO USER ACCESS POLICIES AND PROCEDURES…… 1

2.1 FACTS INFO DATA CLASSIFICATION …….. 1

2.2 ACCESS TO FACTS INFO ……... 2

2.3 ACCOUNT ACCESS AND ROLE REQUESTS…….. 2

2.3.1 FACTS INFO ROLES …… 2

2.3.2 STEPS FOR REQUESTING ACCESS ……... 2

2.3.3 CHANGING ACCESS ROLES ……... 2

2.3.4 DISABLING FACTS INFO USER ACCOUNTS ……... 3

ANNEX 1: FACTS INFO SENSITIVE INFORMATION DISCLOSURE AGREEMENT ……. A1-1

ANNEX 2: FACTS INFO SYSTEM ADMINISTRATIVE RIGHTS AND SENSITIVE INFORMATION DISCLOSURE AGREEMENT ……..…….A2-1

ANNEX 3: PRIVILEGED USER ACCESS AND ACCOUNT MANAGEMENT PROCEDURES….A3-1

1. INTRODUCTION

FACTS Info is an information system created by the Office of the Director of US Foreign Assistance (F) at the Department of State for three primary purposes:

1. Formulation of the foreign assistance budget
2. Collection of budget, operational planning, and performance information
3. Analysis and reporting of data on US foreign assistance programs under the authority of the Director of US Foreign Assistance.

The system collects budget, program, and performance data from the Joint Planning and Performance System and directly from users. FACTS Info is integral in formulating the Foreign Operations Congressional Budget Justification and the Foreign Operations portion of the Annual Performance Report and Annual Performance Plan. Currently FACTS Info contains the following information:

- Budget Data for FY 2006-Present
- FY 2007-Present Operational Plan Data
- FY 2007-Present Performance Plan and Report Data
- FY 2010- Present Mission Strategic and Resource Plan Data

2. FACTS INFO USER ACCESS POLICIES AND PROCEDURES

2.1 FACTS INFO DATA CLASSIFICATION

FACTS Info contains "Sensitive But Unclassified" (SBU) information that must be acquired, maintained and reported in a manner ensuring protection from unauthorized disclosure. SBU information must be handled in accordance with the standards set by:

- Office of Management and Budget (OMB) Circular A-130 Appendix 3;
- The US Department of State Foreign Affairs Manual (including 12 FAM 540);
- The US Agency for International Development (USAID) Automated Directives System (ADS);
- Title 5, United States Code Section 552 (often referred to as "The Freedom of Information Act");
- Title 5, United States Code Section 552a ("The Privacy Act of 1974") for information retrievable by personally identifiable information;
- Procurement Integrity Act (41 USC §423, implemented at FAR 3.104) for procurement sensitive information;
- Other applicable federal laws.

2.2 ACCESS TO FACTS INFO

Access to FACTS Info is controlled through the use of Microsoft Windows Operating System Authentication. To safeguard this data from unauthorized access, both Department of State and USAID security policies require that access be restricted to comply with the above-mentioned laws and regulations. User access is limited to personnel with active United States Government user accounts. Access by any specific individual is at the discretion of F and of the Program Office, Budget Office,

Development Planner, or Bureau Planner of the Operating Unit (OU) to which the individual is assigned. For the purpose of this policy, each OU's Program Office/Budget Office/Development Planner/Bureau Planner is referred to as the OU Approving Officer who receives individual OU user requests and has the ability to authorize those requests. The F approver is referred to as the F Approving Officer. Each OU will establish internal processes and controls to provide appropriate individual access to FACTS Info. All categories of personnel and contractors authorized to view F SBU data are eligible for access to FACTS Info upon approval from F or the OU Approving Officer. Access should be based on need and an understanding of the data contained in the system.

2.3 ACCOUNT ACCESS AND ROLE REQUESTS

2.3.1 FACTS INFO ROLES

Access roles are determined by F and the OU Approving Officer, which have the discretion to provide or withdraw this access at any time. There are two primary types of access to FACTS Info:

- Read Access: The user has data read access for the data contained in FACTS Info, but cannot update or add any data.
- Write Access: The user has modification rights to update or enter data in FACTS Info.

2.3.2 STEPS FOR REQUESTING ACCESS

- All F employees are automatically granted access to FACTS Info. F users' level of access to the system (e.g., Read or Write access) will vary based on the individual user's responsibilities in F and within specific F processes. New F staff should submit a request to F's Information Systems Team (F/IS) via e-mail to activate their access privileges.
- All OU FACTS Info access requests should be submitted to the OU Approving Officer.
- OU Approving Officers will verify, review, and then approve or deny the request within the FACTS Info system based on the user's needs and other appropriate factors.
- Before the OU Approving Officer provides access to a prospective user, the user must read and agree to the FACTS Info confidentiality agreement (See Annexes 1 and 2).
- Users are also strongly encouraged to complete FACTS Info user training. In Washington, this training is arranged by F/IS. Remote training sessions and tutorials by F/IS are available for post users online and within FACTS Info.

2.3.3 CHANGING ACCESS ROLES

Users who need a different access role (for example, changing from read-only to write access) must submit a request to their OU Approving Officer for approval. If the request is approved, the OU Approving Officer will complete the user access role change in FACTS Info. The F Approving Officer will be contacted to execute any changes to permissions requiring administrative access

OU Approving Officers must revise or revoke access to FACTS Info when a user under their authorization transfers, is terminated, or undergoes a substantial change in responsibilities that revises their need for access.

2.3.4 DISABLING FACTS INFO USER ACCOUNTS

OU Approving Officers are responsible for enabling and disabling user accounts. FACTS Info user accounts may be disabled at F's discretion. Reasons for disablement may include:

- User separation from the agency.
- Appearance of user unwillingness or inability to protect sensitive information.

2.3.5 REMOTE USERS ACCESSING FACTS INFO FROM OUTSIDE USG NETWORKS

Additional rules apply to users who access the FACTS Info client from computers that are not resident on a USG network. These rules include the following:

- Any computer with the FACTS Info client installed must also have anti-virus software installed and running, to include the latest anti-virus definitions.
- Any user accessing FACTS Info from outside a USG network must immediately report any suspected security incidents (virus, intrusion, lost/stolen laptop, etc.) that have occurred on their non-USG computer to the FACTS Info Information Systems Security Officer at FACTSInfoSupport@state.gov.
- Any user accessing FACTS Info from outside a USG network must actively log off the system if he/she will be stepping away from his/her computer for any period of time.

ANNEX 1: FACTS INFO SENSITIVE INFORMATION DISCLOSURE AGREEMENT

1. Except as otherwise authorized, access to the FACTS Info database is limited to current employees of USAID and the Department of State, or individuals acting in the capacity of Federal government employees, who have a need to know the information for duties within the scope of their employment.

2. By accessing FACTS Info, I understand and agree to the provisions stated below with regard to the FACTS Info data system.

- Some information contained in the FACTS Info data system is considered to be sensitive but unclassified, and I will treat it as such. This could include preliminary and planning information, business-confidential information protected by the Trade Secrets Act, or information protected by the Privacy Act of 1974.
- I will not knowingly disclose sensitive information, including procurement sensitive information, directly or indirectly to any person other than a person authorized to receive or have access to such information. I understand that unauthorized disclosure of such information may subject me to administrative disciplinary action and/or to civil and criminal penalties, including fines, imprisonment, and loss of employment under the Procurement Integrity Act or other applicable laws and regulations. I will promptly refer any questions or concerns regarding compliance to the appropriate agency procurement, ethics, or legal official(s).
- I will not release information contained in FACTS Info outside of the Department of State and the U.S. Agency for International Development without advance clearance by my F Point of Contact (F POC) as mandated by Section 6 of the FACTS and FACTS Info Data Use Policy.
- I will notify the FACTS Info ISSO immediately in the event of suspected lost or compromised credentials. The ISSO is then responsible for ensuring that the credentials are changed and the security incident is investigated.
- I will immediately notify the OU Approving Officer in the event that my employment status or Operating Unit assignment is changed.

ANNEX 2: FACTS INFO SYSTEM ADMINISTRATIVE RIGHTS AND SENSITIVE INFORMATION DISCLOSURE AGREEMENT

1. Except as otherwise authorized, access to the FACTS Info database is limited to current employees of USAID and the Department of State, or individuals acting in the capacity of Federal government employees, who have a need to know the information for duties within the scope of their employment.

2. By accessing FACTS Info, I understand and agree to the provisions stated below with regard to the FACTS Info data system.

- Some information contained in the FACTS Info data system is considered to be sensitive but unclassified, and I will treat it as such. This could include preliminary and planning information, business-confidential information protected by the Trade Secrets Act, or information protected by the Privacy Act of 1974.
- I will not knowingly disclose sensitive information, including procurement sensitive information, directly or indirectly to any person other than a person authorized to receive or have access to such information. I understand that unauthorized disclosure of such information may subject me to administrative disciplinary action and/or to civil and criminal penalties, including fines, imprisonment, and loss of employment under the Procurement Integrity Act or other applicable laws and regulations. I will promptly refer any questions or concerns regarding compliance to the appropriate agency procurement, ethics, or legal official(s).
- I will not release information contained in FACTS Info outside of the Department of State and the U.S. Agency for International Development without advance clearance by my F Point of Contact (F POC) as mandated by Section 6 of the FACTS and FACTS Info Data Use Policy.
- Privileged users are aware that the FACTS Info ISSO should be notified immediately in the event of suspected lost or compromised credentials. The ISSO is then responsible for ensuring that the credentials are changed and the security incident is investigated.
- The FACTS Info ISSO will be immediately notified upon any changes in the status or roles of privileged user accounts.

3. By utilizing administrative rights to FACTS Info, I acknowledge that I will only use the assigned privileges for purposes of system development, user administration, training and demonstrations, editing code, compiling code, and operating the system in compliance with the FACTS Program Data Access and Use Policy, the FACTS Info User Access Policy, and the requirements of my position.

FACTS Info User: Signature_____ Date_____

FACTS Info ISSO: Signature_____ Date_____

F/PM/IS Lead: Signature_____ Date_____

ANNEX 3: PRIVILEGED USER ACCESS AND ACCOUNT MANAGEMENT PROCEDURES

This process describes account management for privileged users of FACTS Info. This includes users with accounts at the operating system, database, and application level that have privileges above that of a regular end user of FACTS Info. This process addresses distribution and revocation of these accounts, as well as the process for handling lost or compromised credentials.

The process for requesting, distributing, revoking, and recertifying these users' accounts is based on State/F established procedures. Privileged users are required to complete the end user access request form to collect each user's basic information and document the user's justification for access. When submitting a request for access, privileged users should indicate and justify the need for an elevated level of access. Annex 2 documents the type of access the user requires and justification for access. All privileged users are State or USAID employees and/or contractors and must hold a minimum Secret clearance.

Once completed, the form is sent to the FACTS Info ISSO for review, who will then forward the form to the F/IS Team Lead for final approval. The ISSO will track all of the access request forms and once access has been approved, he/she manages distribution and revocation of access. This includes securely transmitting the initial credentials to the new user. On a yearly basis, the ISSO will certify that all privileged users still require the same level of access to perform their job functions. If access is no longer required, the ISSO will initiate a request to revoke the access, which must be approved by the F/IS Team Lead.

The ISSO will maintain supervision for privileged user account management for the application, operating systems, and database used as part of FACTS Info. Management of these user accounts will comply with the following minimum configuration requirements:

- Outdated/unused accounts will be detected and disabled or removed annually.
- At a minimum, each privileged account will be reviewed annually to ensure the elevated access permissions are still necessary.
- Any service and application accounts will have passwords changed annually at a minimum or when any member of the administrative team leaves the organization.
- Passwords for administrator-level accounts will be changed at least every 90 days or when any member of the administrative team leaves the organization.
- Privileged users should notify the FACTS Info Information Systems Security Officer (ISSO) immediately in the event of suspected lost or compromised credentials. The ISSO is then responsible for ensuring that the credentials are changed and the security incident is investigated.

The FACTS Info ISSO should be immediately notified upon any changes in the status or roles of privileged user accounts.